

Amendments to the Claims:

Please amend the claims as indicated.

1. (Currently amended) An apparatus for authorized remote access to a target system,
the apparatus comprising:

a security module comprising executable code stored on a storage device, executed
by a processor, and configured to selectively generate an encrypted key in
response to a first password and communicate the encrypted key to a remote
system and establish a remote communication connection between a remote
system and a target system in response to a third password; and

an authorization module comprising executable code stored on the storage device,
executed by the processor, and configured to receive the encrypted key and
a second password from the remote system, decrypt the encrypted key, and
determine ~~at~~ the third password in response to authenticating ~~[[a]]~~ the second
password and identifying a remote user of the remote system within an
authorized user list, and communicate the third password to the remote
system[[.]]; and

the security module further configured to establish a remote communication
connection between the remote system and the target system in response to
receiving the third password from the remote system.

2. (Original) The apparatus of claim 1, wherein the first password determines a set of commands available to the remote user logged into the target system, the commands organized according to a plurality of hierarchical access levels.

3. (Original) The apparatus of claim 1, wherein the third password is operable for only a selected period of time.

4. (Currently amended) The apparatus of claim 1, wherein the authorization module is configured to communicate with the[[a]] remote user ~~connected~~ over a secure communication link between the remote system andwith the authorization module, and the authorization module is physically remote from the security module.

5. (Currently amended) The apparatus of claim 1, wherein [[a]]the remote user is conditionally added to the authorized user list upon completion of a remote application process.

6. (Currently Amended) The apparatus of claim 1, further comprising an update module comprising executable code stored on the storage device, executed by the processor, and configured to compare the authorized user list to a master list of personnel potentially authorized for remote access to the target system and to selectively remove remote users from the authorized user list not found on the master list.

7. (Currently amended) The apparatus of claim 1, wherein the security module and authorization module comprise a log module comprising executable code stored on the storage device, executed by the processor, and configured to log actions of the remote user communicating

communicating with the target system and the authorization module.

8. (Currently amended) An apparatus for authorized remote access to a target system, the apparatus comprising:

a login module comprising executable code stored on a storage device, executed by a processor, and configured to establish communications with a remote user in response to a personal user identifier and a secondpersonal password;

a confirmation module comprising executable code stored on the storage device, executed by the processor, and configured to determine whether the remote user is identified within an authorized user list;

a decryption module comprising executable code stored on the storage device, executed by the processor, and configured to decrypt an encrypted key provided by the remote user in response to identification of the remote user within the authorized user list, the encrypted key sent to the remote user by a target system in response to a ~~first~~^{[[n]]} ~~access level~~ password received from the remote user;

a password module comprising executable code stored on the storage device, executed by the processor, and configured to derive a ~~third~~^{temporary} password from a decrypted version of the encrypted key and communicate the third password to the remote user, wherein the remote user employs the

third password to establish a remote communication connection between the remote system and the target system.

9. (Currently amended) The apparatus of claim 8, wherein the ~~first~~access level password defines a set of commands available to the remote user logged into the target system, the commands organized according to a plurality of hierarchical access levels.

10. (Currently amended) The apparatus of claim 8, wherein the ~~third~~temporary password is operable for a selected period of time.

11. (Currently amended) The apparatus of claim 8, wherein the authorization module is configured to communicate with ~~[[a]]the remote user connected remotely to the apparatus~~ over a secure communication link.

12. (Original) The apparatus of claim 8, wherein an authorized remote user is conditionally added to the authorized user list in response to approval from at least two supervisors of the user upon completion of a remote application process.

13. (Currently amended) The apparatus of claim 8, further comprising an update module comprising executable code stored on the storage device, executed by the processor, and configured to compare the authorized user list to a master list of personnel potentially authorized for remote access to the target system and to selectively remove remote users from the authorized user list not found on the master list.

14. (Currently amended) The apparatus of claim 8, further comprising a log module comprising executable code stored on the storage device, executed by the processor, and configured to log communications between the remote user and the apparatus.

15. (Currently amended) A system for authorized remote access to a target system, comprising:

a target system configured to selectively generate an encrypted key in response to a first password received from a remote system and communicate the encrypted key to the remote system ~~and establish a remote communication connection with a remote system in response to a third password;~~

an authorization server remote from the target system and the remote system, the authorization server configured to receive the encrypted key and a second password from the remote system, decrypt the encrypted key and determine ~~at~~ the third password in response to authenticating ~~[[a]]~~ the second password and identifying a remote user of the remote system within an authorized user list, the authorization server configured to then send the third password to the remote system ~~[[.]]; and~~

the target system further configured to establish a remote communication connection with the remote system in response to the third password received from the remote system.

16. (Original) The system of claim 15, wherein the first password determines a set of commands available to a remote user remotely accessing the target system.

17. (Original) The system of claim 15, wherein the third password is operable for a limited time period.

18. (Currently amended) The system of claim 15, wherein ~~the an authorized~~ remote user ~~associated with the second password~~ is conditionally added to the authorized user list upon completion of a remote application process.

19. (Currently amended) The system of claim 15, further comprising an update module comprising executable code stored on a storage device, executed by a processor, and configured to compare the authorized user list to a master list of personnel potentially authorized for remote access to the target system and to selectively remove remote users from the authorized user list not found on the master list.

20. (Original) The system of claim 15, wherein the target system and authorization server are configured to log actions of a user of the remote system.

21. (Original) The system of claim 15, wherein the target system comprises a data storage system.

22. (Currently amended) A method for authorized remote access to a target system, comprising:
- retrieving an encrypted key from a target system accessed by way of a first password;
 - connecting to an authorization module using a second password ~~[[I]]~~in order to retrieve a third password associated with the encrypted key, the authorization module selectively decrypting the encrypted key in response to determining that a remote user is identified within an authorized user list, wherein the authorization module is physically remote from the target system; and
 - logging into the target system using the third password.
23. (Original) The method of claim 22, wherein the first password determines a set of commands available to the remote user logged into the target system, the commands organized according to a plurality of hierarchical access levels.
24. (Original) The method of claim 22, wherein the third password is operable for a limited time period.
25. (Currently amended) The method of claim 22, wherein the remote user communicates over a secure communication link to the authorization module ~~that is physically remote from the target system.~~

26. (Currently amended) The method of claim 22, further comprising completing a remote access application process that conditionally adds ~~[[a]]~~the remote user to the authorized user list.

27. (Original) The method of claim 22, further comprising comparing the authorized user list to a master list of personnel potentially authorized for remote access to the target system and selectively removing remote users from the authorized user list not found on the master list.

28. (Original) The method of claim 22, further comprising logging actions of the remote user communicating with the target system and the authorization module.

29. (Currently amended) A method for authorized remote access to a target system, comprising:

 sending an encrypted key to a remote system in response to authenticating a remote user using a first password;

 connecting ~~to the remote system~~user in response to the remote user entering a third password associated with the encrypted key, the third password provided to the remote user logged into an authorization module using a second password, the authorization module selectively decrypting the encrypted key received from the remote user in response to determining that the remote user is identified within an authorized user list.

30. (Currently amended) The method of claim 29, wherein the first password determines a set of commands available to the remote user logged into ~~[[a]]the~~ target system, the commands organized according to a plurality of hierarchical access levels.

31. (Original) The method of claim 29, wherein the third password is operable for a limited time period.

32. (Currently amended) The method of claim 29, further comprising completing a remote access application process that conditionally adds ~~[[a]]the remote~~ user to the authorized user list.

33. (Original) The method of claim 29, further comprising comparing the authorized user list to a master list of personnel potentially authorized for remote access to the target system and selectively removing remote users from the authorized user list not found on the master list.

34. (Original) The method of claim 29, further comprising logging actions of the remote user communicating with the authorization module and a target system.

35. (Currently amended) An apparatus for authorized remote access to a target system, comprising:

means for retrieving an encrypted key from a target system accessed by way of a first password, the retrieving means comprising executable code stored on a storage device and executed by a processor;

means for connecting to an authorization module using a second password to retrieve a third password associated with the encrypted key, the authorization module selectively decrypting the encrypted key in response to determining that a remote user is identified within an authorized user list, the connecting means comprising executable code stored on the storage device and executed by the processor; and means for logging into the target system using the third password, the logging means comprising executable code stored on the storage device and executed by the processor.

36. (Original) The apparatus of claim 35, wherein the first password determines a set of commands available to the remote user logged into the target system, the commands organized according to a plurality of hierarchical access levels.

37. (Currently amended) The apparatus of claim 35, further comprising means for logging actions of the remote user communicating with the target system and the authorization module, the remote logging means comprising executable code stored on the storage device and executed by the processor.

38. (Original) An article of manufacture comprising a program storage medium readable by a processor and embodying one or more instructions executable by a processor to perform a method for authorized remote access to a target system, the method comprising:

retrieving an encrypted key from a target system accessed by way of a first password;

connecting to an authorization module using a second password to retrieve a third password associated with the encrypted key, the authorization module selectively decrypting the encrypted key in response to determining that a remote user is identified within an authorized user list; and logging into the target system using the third password

39. (Original) The article of manufacture of claim 38, wherein the first password determines a set of commands available to the remote user logged into the target system, the commands organized according to a plurality of hierarchical access levels.

40. (Original) The article of manufacture of claim 38, further comprising logging actions of the remote user communicating with the target system and the authorization module.